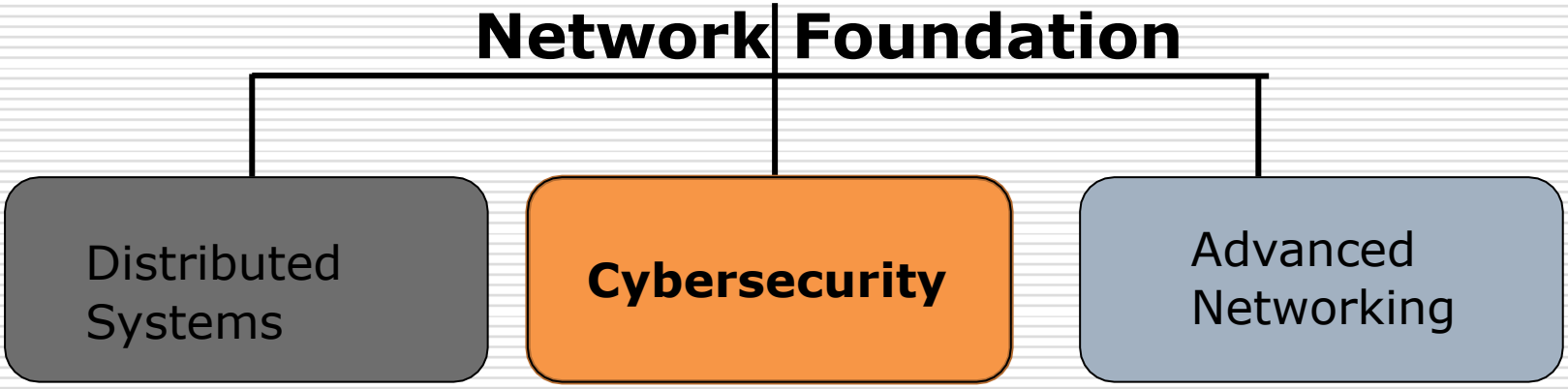
Introduction to Computer and Network Security

By : Pr RIAHLA

Computer Networking Prerequisites



- TCP/IP Recap
- Client-Server (FTP, Telnet, SSH, …)
- Sockets
- NFS (Network File System)
- RPC, CORBA, RMI
- Distributed Algorithms

- Advanced Routing
- Dynamic Networks:
- Ad Hoc Networks
- Peer-to-Peer (P2P) Networks

Program

4 parts

I. Introduction to Cybersecurity

II. Threats (Attacks, and Vulnerabilities)

III. Protections

IV. Security Management

4 parts

I. Introduction to Cybersecurity

II. Threats (Attacks, and Vulnerabilities)

III. Protections

IV. Security Management

Introduction to Cybersecurity

- Introduction (General Overview and History)
- Fundamental Security Requirements and Objectives
- Risk Assessment
- Establishing a Security Policy
- Elements of a Security Policy
- Major Security Flaws
- Audit Concept

4 parts

I. Introduction to Cybersecurity

II. Threats (Attacks, and Vulnerabilities)

III. Protections

IV. Security Management

Threats (Security Flaws, Attacks, and Vulnerabilities)

- Introduction
- Different Types of Vulnerabilities
- Viruses,
- Worms,
- Trojans, and Others
- Application Vulnerabilities
- Network Vulnerabilities
- Espionage

4 parts

I. Introduction to Cybersecurity

II. Threats (Attacks, and Vulnerabilities)

III. Protections

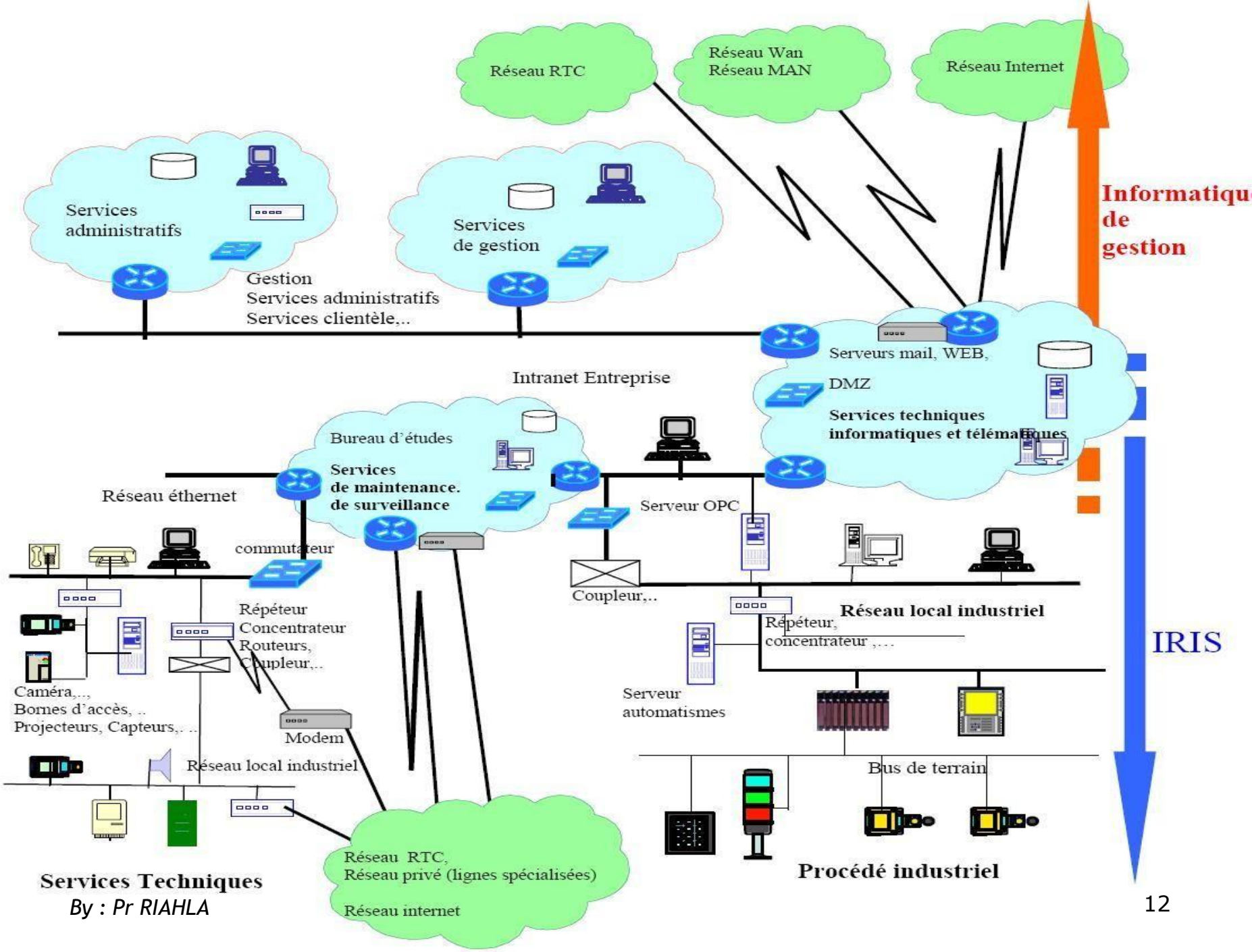
IV. Security Management

Cryptography

- Classical Cryptography
- Symmetric Cryptography
- Asymmetric Cryptography
- Hybrid Encryption
- Digital Signature and Certificate
- PKI (Public Key Infrastructure)
- Secure Communications and Applications

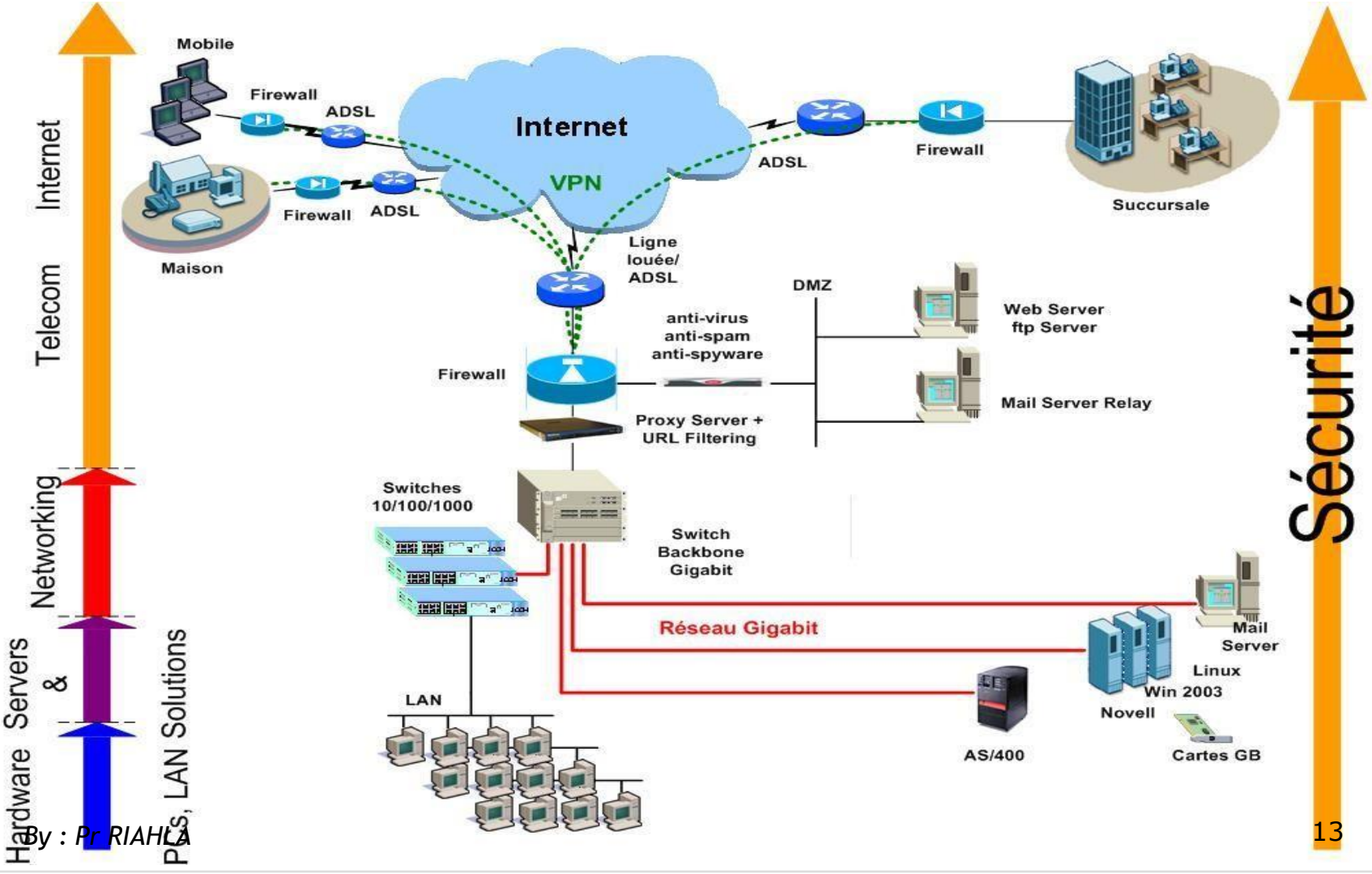
Protections

- User Training
- Workstation
- Antivirus
- Authentication and Encryption
- Firewall: Translation, Filtering, and Proxies
- Intrusion Detection
- Secure Communications and Applications
- VPNs (Virtual Private Networks)


Réseau RTC
Réseau Wan
Réseau MAN
Réseau Internet
Informatique de gestion
Services administratifs
Services de gestion
Gestion
Services administratifs
Services clientèle,..
Intranet Entreprise
Serveurs mail, WEB,
DMZ
Services techniques informatiques et télématiques
Bureau d'études
Services de maintenance. de surveillance
Réseau éthernet
commutateur
Serveur OPC
Coupleur,..
Réseau local industriel
Répéteur, concentrateur ,...
Répéteur
Concentrateur
Routeurs,
Coupleur,..
Caméra,..,
Bornes d'accès, ..
Projecteurs, Capteurs,. ..
Modem
Serveur automatismes
Réseau local industriel
Bus de terrain
IRIS
Réseau RTC,
Réseau privé (lignes spécialisées)
Réseau internet
Services Techniques
Procédé industriel

By : Pr RIAHLA

Protections



4 parts

I. Introduction to Cybersecurity

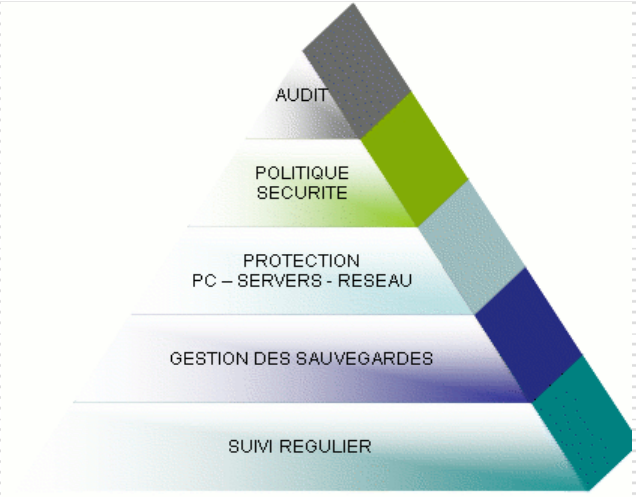
II. Threats (Attacks, and Vulnerabilities)

III. Protections

IV. Security Management

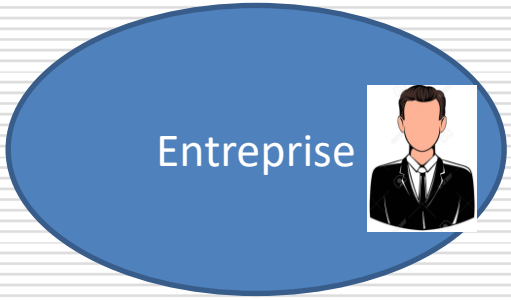
Security Management

- Definition of a Security Policy
- Security Standards and Guidelines
- Audit
- ISO XX XXX Certification



Cybersecurity Profession

- **Beginner in Information Security (SSI):** €32,000 per year --- €3,000 per month
- **CISO (Chief Information Security Officer)**: €70,000 per year --- €6,000 per month



- **Expert Consultant**: €600 per day --- €18,000 per month or more!

I. Introduction to Cybersecurity

Introduction (History)

Introduction (History) (Kevin mitnick)

U.S. Department of Justice
United States Marshals Service

WANTED
BY U.S. MARSHALS

NOTICE TO ARRESTING AGENCY: Before arrest, validate warrant through National Crime Information Center (NCIC).

United States Marshals Service NCIC entry number: (NIC/ W721460921).

NAME: .....MITNICK, KEVIN DAVID

AKS (S): .....MITNIK, KEVIN DAVID
MERRILL, BRIAN ALLEN

DESCRIPTION:

Sex: .....MALE
Race: .....WHITE
Place of Birth: .....VAN NUYS, CALIFORNIA
Date(s) of Birth: 08/06/63; 10/18/70
Height: .....5'11"
Weight: 190
Eyes: .....BLUE
Hair: .....BROWN
Skintone: .....LIGHT
Scars, Marks, Tattoos: .....NONE KNOWN
Social Security Number (s): 550-39-5695
NCIC Fingerprint Classification: ...DOPM20PM13DIPM19PM09

ADDRESS AND LOCALE: KNOWN TO RESIDE IN THE SAN FERNANDO VALLEY AREA OF CALIFORNIA AND LAS VEGAS, NEVADA

WANTED FOR: VIOLATION OF SUPERVISED RELEASE
ORIGINAL CHARGES: POSSESSION UNAUTHORIZED ACCESS DEVICE; COMPUTER FRAUD
Warrant Issued: CENTRAL DISTRICT OF CALIFORNIA
Warrant Number: 9312-1112-0154-C

DATE WARRANT ISSUED: NOVEMBER 10, 1992

MISCELLANEOUS INFORMATION: SUBJECT SUFFERS FROM A WEIGHT PROBLEM AND MAY HAVE EXPERIENCED WEIGHT GAIN OR WEIGHT LOSS
VEHICLE/TAG INFORMATION: NONE KNOWN OFTEN USES PUBLIC TRANSPORTATION

If arrested or whereabouts known, notify the local United States Marshals Office, (Telephone: 213-894-2485).

If no answer, call United States Marshals Service Communications Center in McLean Virginia.
Telephone (800)336-0102 (24 hour telephone contact) NLETS access code is VAUSM0000.

PRIOR EDITIONS ARE OBSOLETE AND NOT TO BE USED

Form USM -132
(Rev. 3/2/82)

November 1992

Introduction (History) (Kevin mitnick)

- He started hacking telephone networks.
- He attacked the machines of Tsutomu Shimomura at the Supercomputing Center.

- He penetrated the WELL servers and accessed Markoff's (a journalist's) emails.

- He was arrested with the help of an announcement by Shimomura and the WELL organization.

- He served 5 years in prison and was banned from using computers for 2 years.

Introduction (History) (Kevin mitnick)

- He has been a cybersecurity consultant since 2000.
- He published a book covering social engineering, IDS (Intrusion Detection Systems), and more.

History (DDoS)

February 2000
Several major websites were inaccessible (eBay, CNN, Amazon, Microsoft, ...) for several hours.They were flooded by a massive traffic flow (up to 1 Gbps) from multiple addresses.

February 16th, someone is suspected of launching the attacks.

April 15th, he is arrested in Canada, he is 15 years old.

History (DDoS)

He was sentenced to 8 months in a detention center.

With an automated program, he was able to hack 75 different machines due to a vulnerability in their FTP servers.

He installed a distributed attack program (DDoS) on these machines.

History (DDoS)

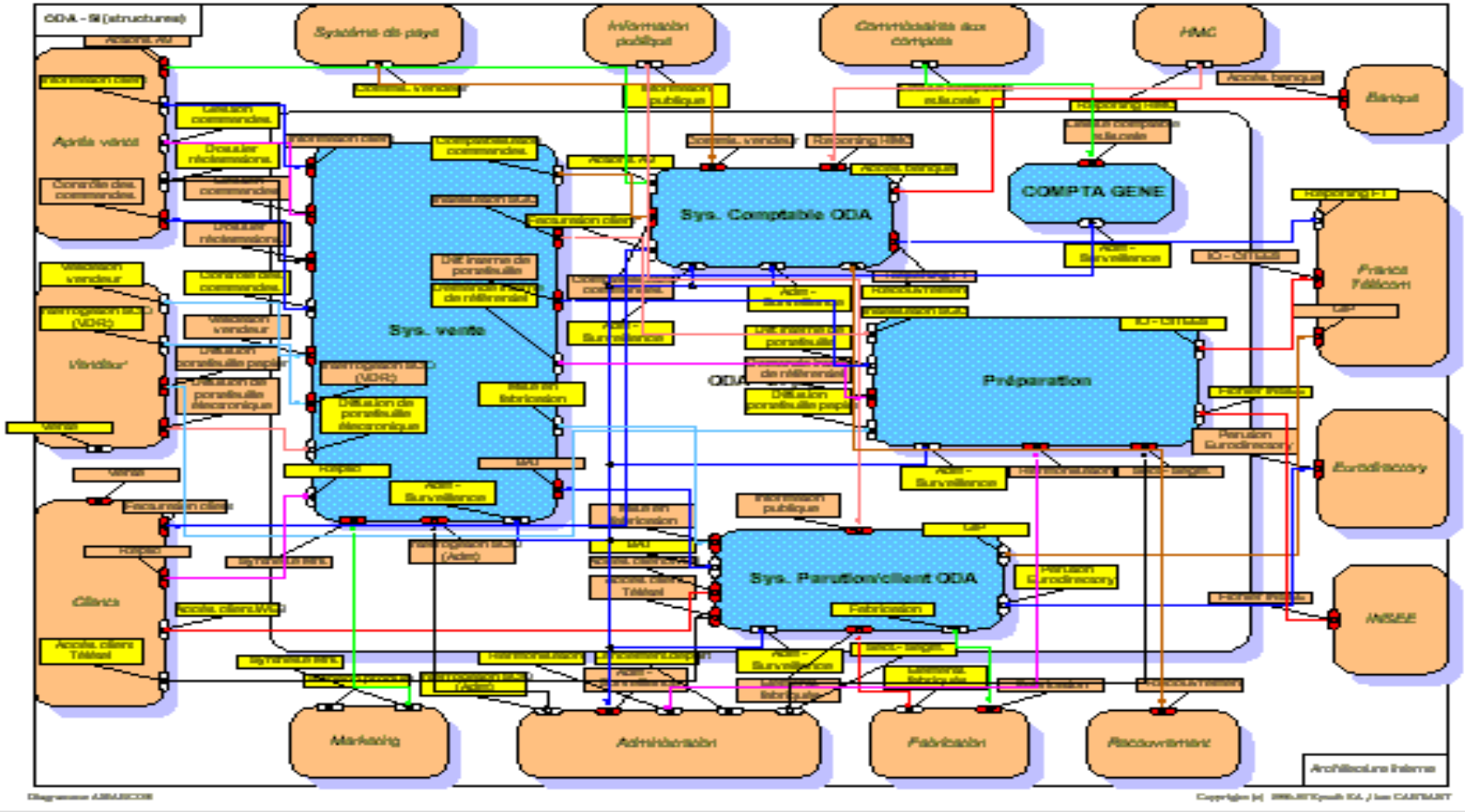
- MELLISA and Other Bugs
- Remote Banking Operation Program
- Viruses, Worms, Spyware, …
- Network Attacks
- …

Information Systems

- An information system is generally defined as the collection of data and the hardware and software resources of a company that allow them to be stored or circulated

- Organization of activities aimed at acquiring, storing, transforming, distributing, exploiting, managing... information.

Information Systems



Information Systems

Increasing need for information

Information Systems

- Great diversity in the nature of information:
- Financial data
- Technical data
- Medical data…

These data constitute the assets of individuals and companies and can be highly coveted.

Computer Systems

- One of the technical means to operate an information system is to use a computer system (core).

- **"Computer systems have become the target of those who covet information.**

Ensuring information security => ensuring the security of computer systems.

Cybersecurity:
Information Security

- With the development of internet usage, more and more companies are opening their information systems to their partners or suppliers.

It is therefore essential to know the resources of the company to protect and to control access and the rights of the users of the information system.

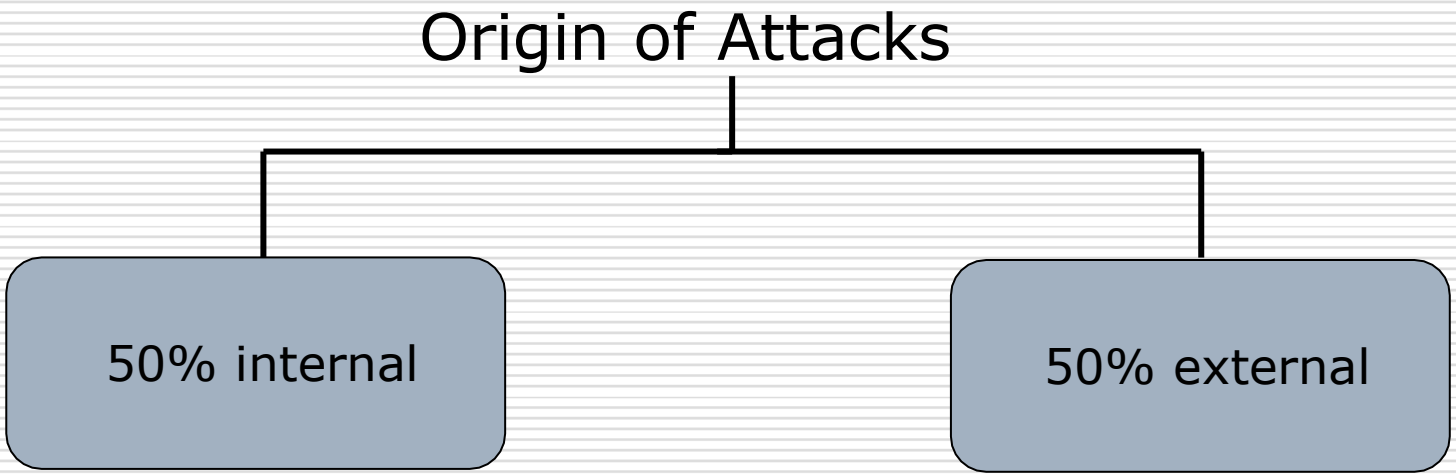
Cybersecurity: Information Security

Cybersecurity is the set of measures implemented to reduce the vulnerability of a system against accidental or intentional threats.

Cybersecurity: Information Security

Fundamental Requirements and Objectives

Fundamental Requirements and Objectives



Example: malicious user, unintentional error, ...

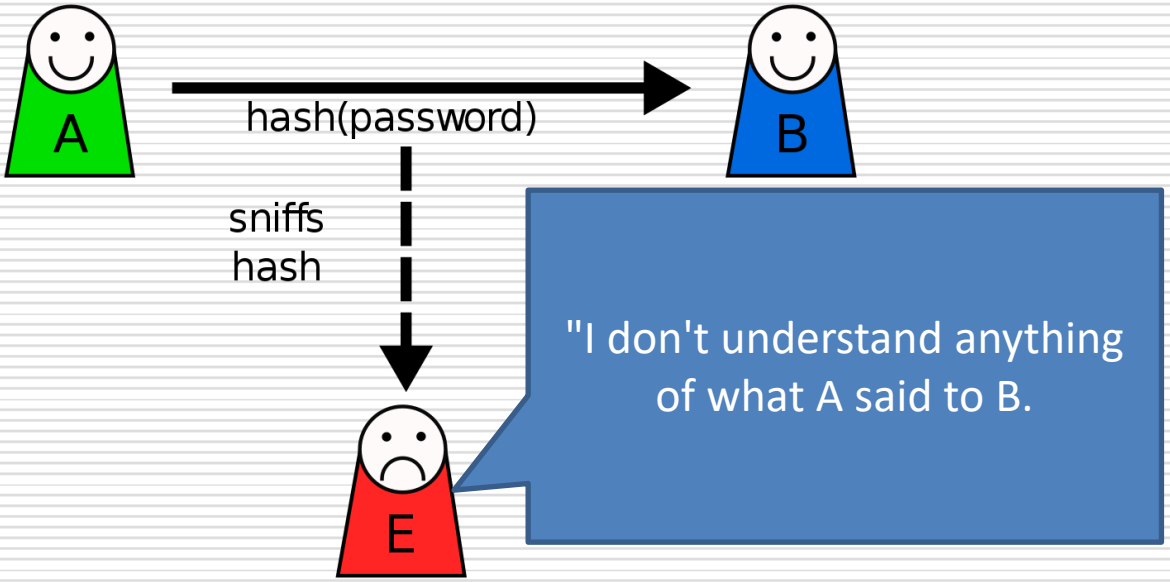
Example: Hacking, viruses, intrusion, ...

Fundamental Requirements and Objectives

- They define what users of the information system expect in terms of security.

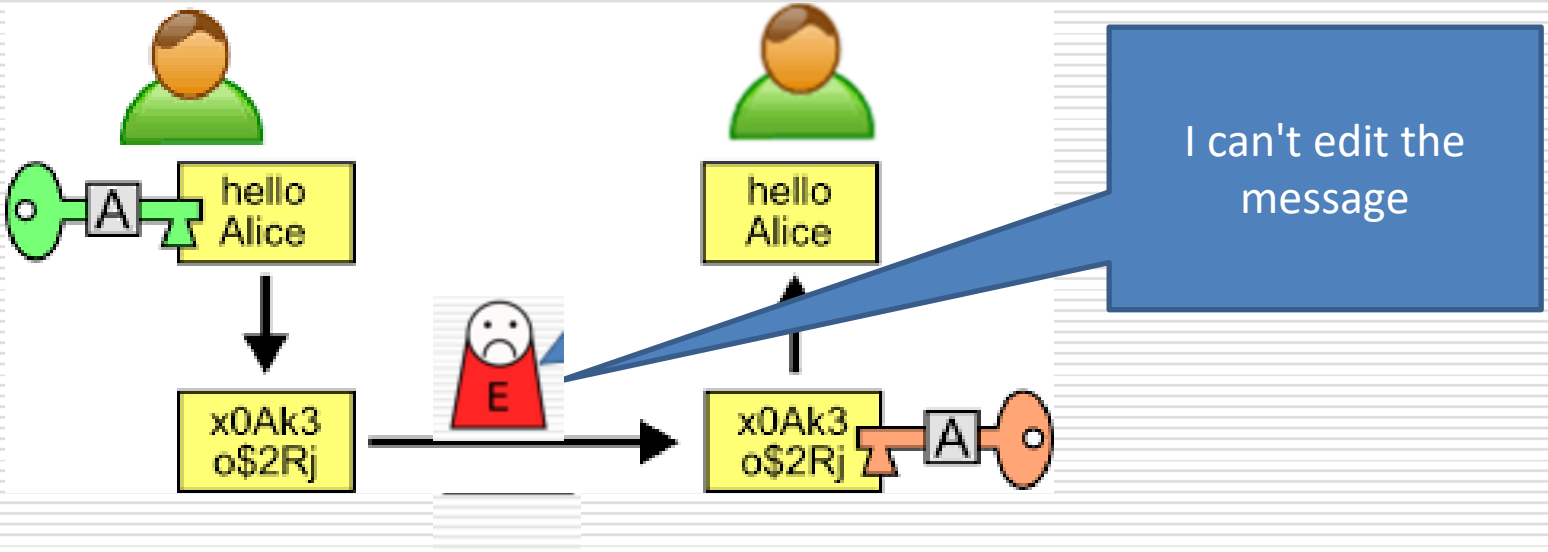
Fundamental Requirements and Objectives

➢**Confidentiality,** ensuring that only authorized individuals have access to the exchanged resources



Fundamental Requirements and Objectives

➢**Integrity,** meaning ensuring that the data is indeed what it is believed to be.



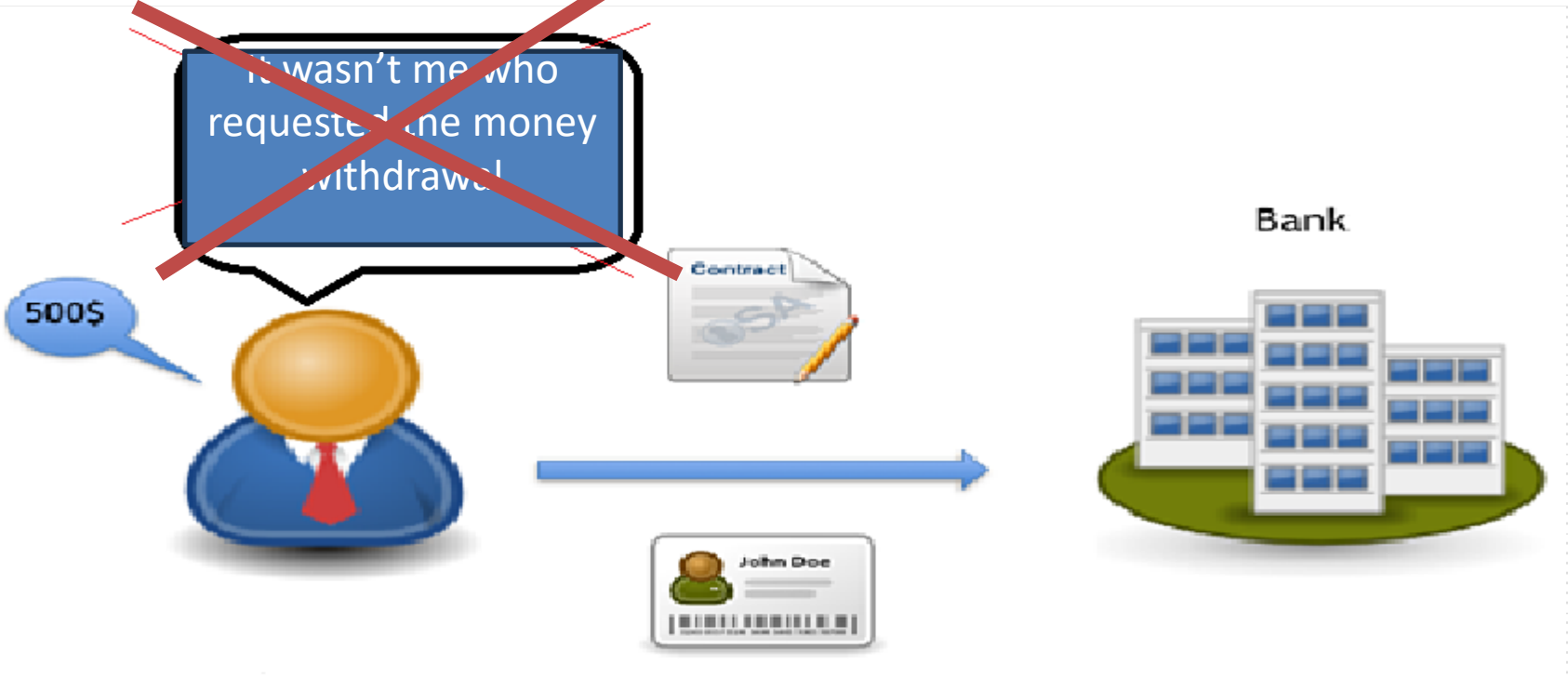
The information has not been altered between its creation and its processing (and transfer).

Fundamental Requirements and Objectives

➢**Availability,** ensuring the proper functioning of the information system

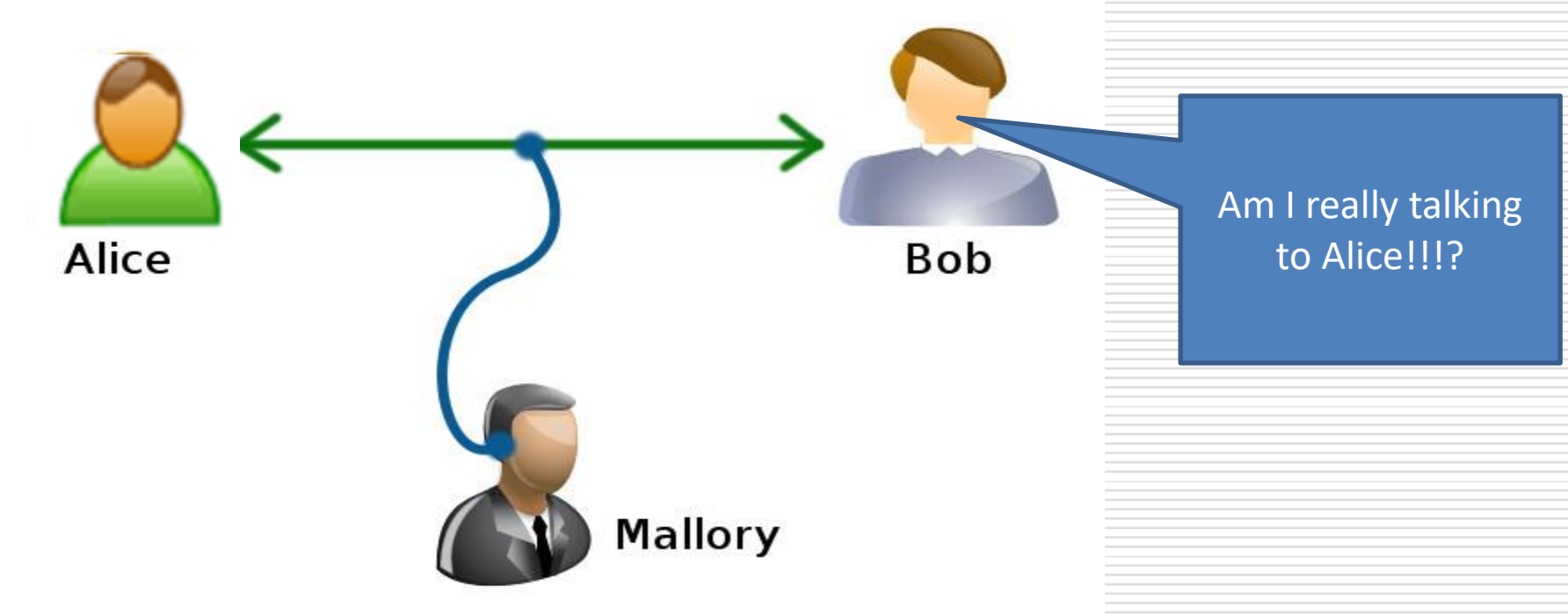
Fundamental Requirements and Objectives

Non-repudiation, ensuring that a transaction cannot be denied**.**



Fundamental Requirements and Objectives

Authentication, ensuring that only authorized individuals have access to the resources.



Fundamental Requirements and Objectives

Authentication

What I have

What I know

What I am

Fundamental Requirements and Objectives

Respect for privacy

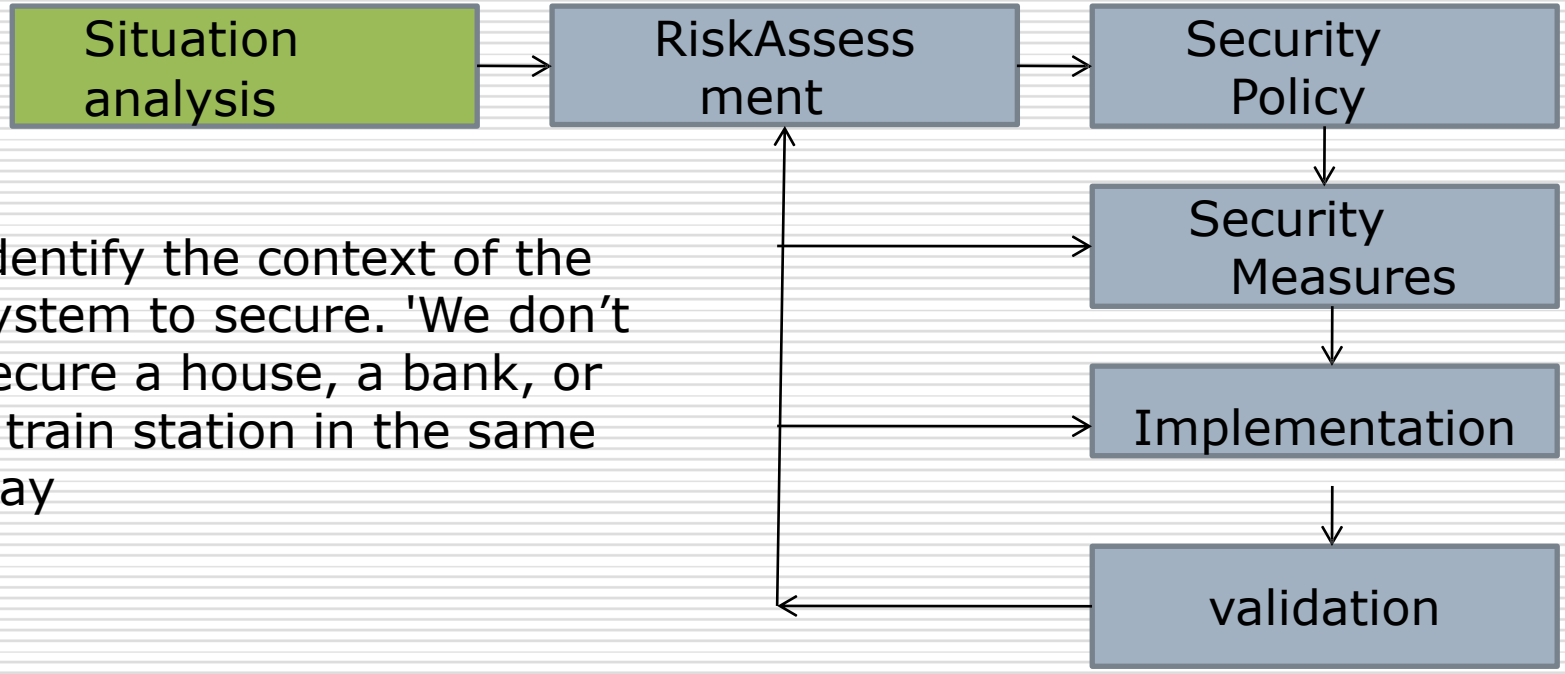
And others…

- Eligibility
- Usefulness
- …

Approach (Methodology?) to secure an information system

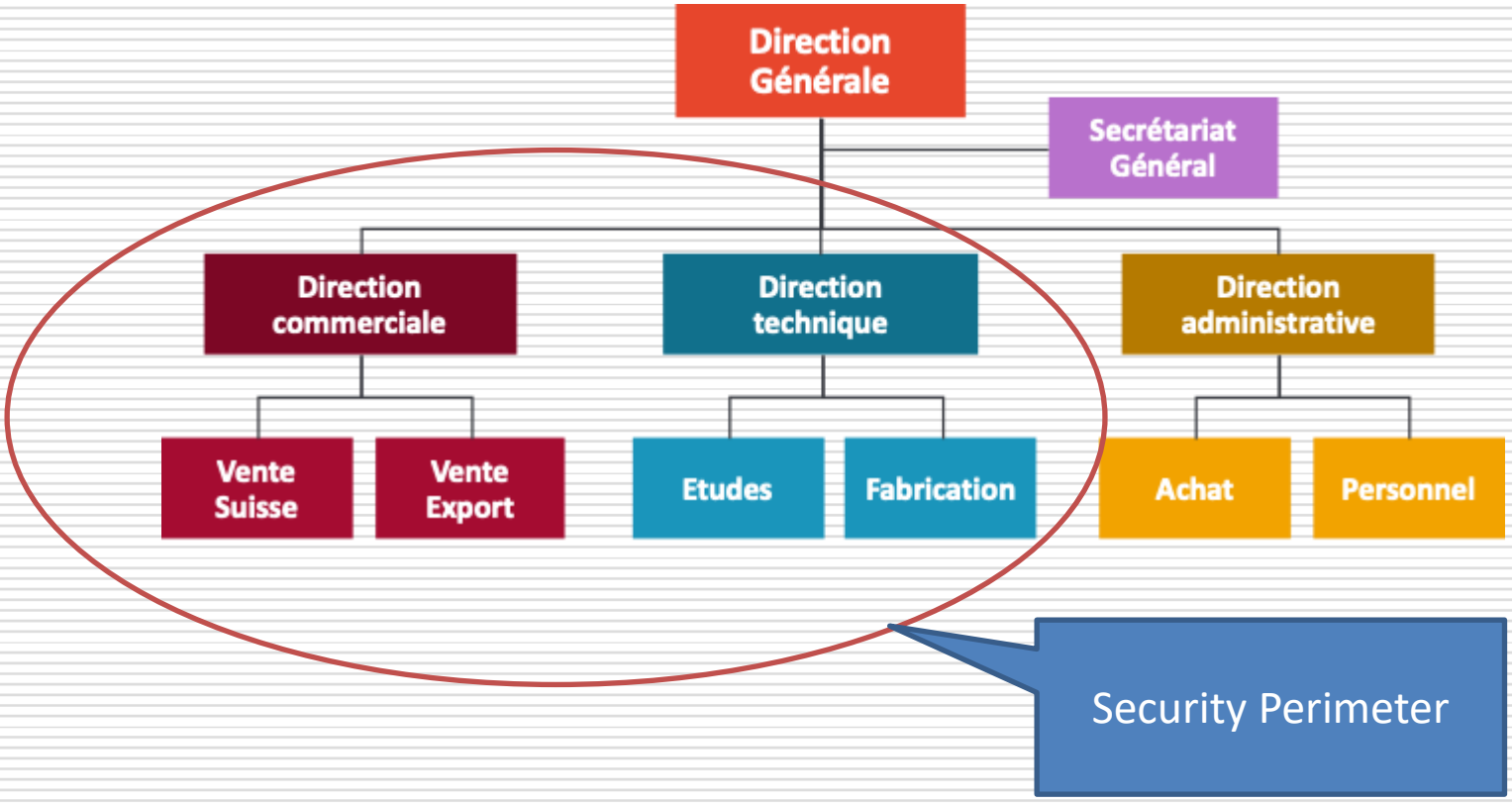
Approach (Methodology?) to secure an information system

Approach (Methodology?) to secure an information system



Identify the context of the system to secure. 'We don’t secure a house, a bank, or a train station in the same way

Approach (Methodology?) to secure an information system

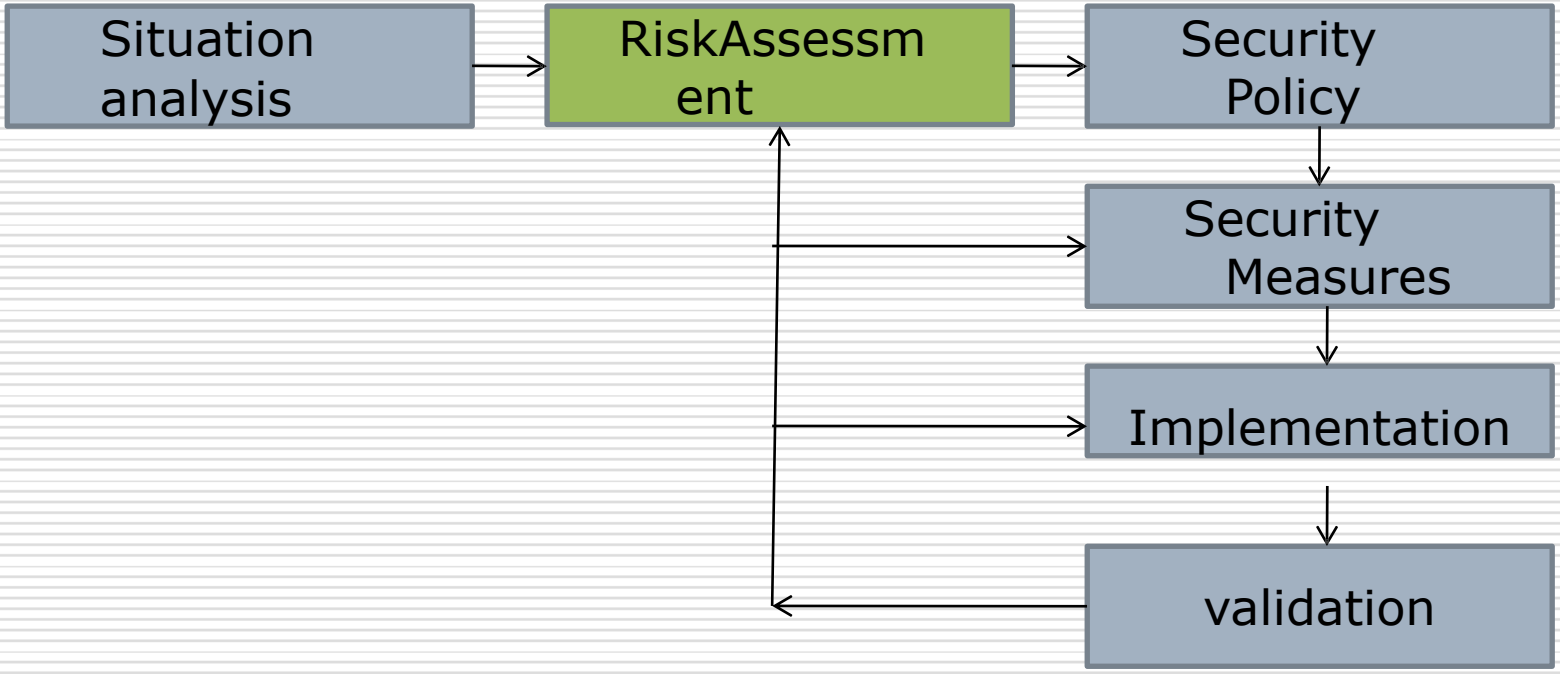


Approach (Methodology?) to secure an information system

Approach (Methodology?) to secure an information system

Risk Assessment

Approach (Methodology?) to secure an information system



Approach to securing an IS - Risk Assessment

- It is necessary to conduct a risk assessment while carefully identifying potential issues, along with solutions and associated costs.

- The set of selected solutions must be organized into a coherent security policy, depending on the level of risk tolerance.

Approach to securing an IS - Evolution of Risks

- Growth of the Internet
- Increase in Attacks
- Vulnerabilities in Technologies
- Vulnerabilities in Configurations
- Weaknesses in Security Policies
- Changing Profile of Hackers

Approach to securing an IS - Risk Assessment

- What is the value of equipment, software, and especially information?
- What is the cost and the replacement time?
- Conduct a vulnerability analysis of the information contained on networked computers (packet analysis tools, logs, etc.).
- What would be the impact on customers of public information regarding intrusions into the company's computers?

Approach to securing an IS - Risk Assessment

However, it is important to be aware that the main risks remain:

- Cut cable"
- "Power outage"
- "Disk crash"

➢ ...

Risk Analysis (Study) - Key Takeaways

1. Inventory of system elements to protect
2. Inventory of possible threats (incidents) to these elements
3. Estimation of the probability of these threats occurring
4. Estimation of the cost associated with each incident

Risk Analysis (Study) - Key Takeaways

	High Cost	Low Cost
Frequent Incidents	Incident Incident Incident …	Incident Incident Incident …
Rare Incidents	Incident Incident Incident …	Incident Incident Incident …

Risk Analysis (Study) - Key Takeaways

	High Cost	Low Cost
Frequent Incidents	• **Implement security mechanisms** • **Recruit** • **Train...**	
Rare Incidents		

Risk Analysis (Study) - Key Takeaways

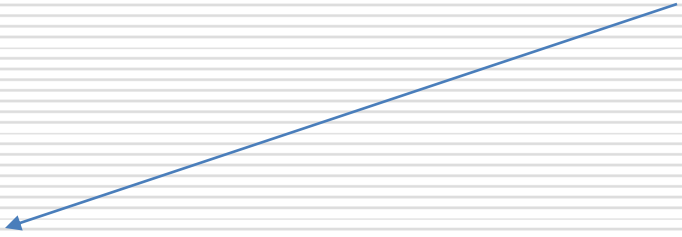
	High Cost	Low Cost
Frequent Incidents	• **Implement security mechanisms** • **Recruit** • **Train...**	Ensure availability (mirror servers, etc.)
Rare Incidents		

Risk Analysis (Study) - Key Takeaways

	High Cost	Low Cost
Frequent Incidents	• **Implement security mechanisms** • **Recruit** • **Train...**	Ensure availability (mirror servers, etc.)
Rare Incidents	Ensure	

Risk Analysis (Study) - Key Takeaways

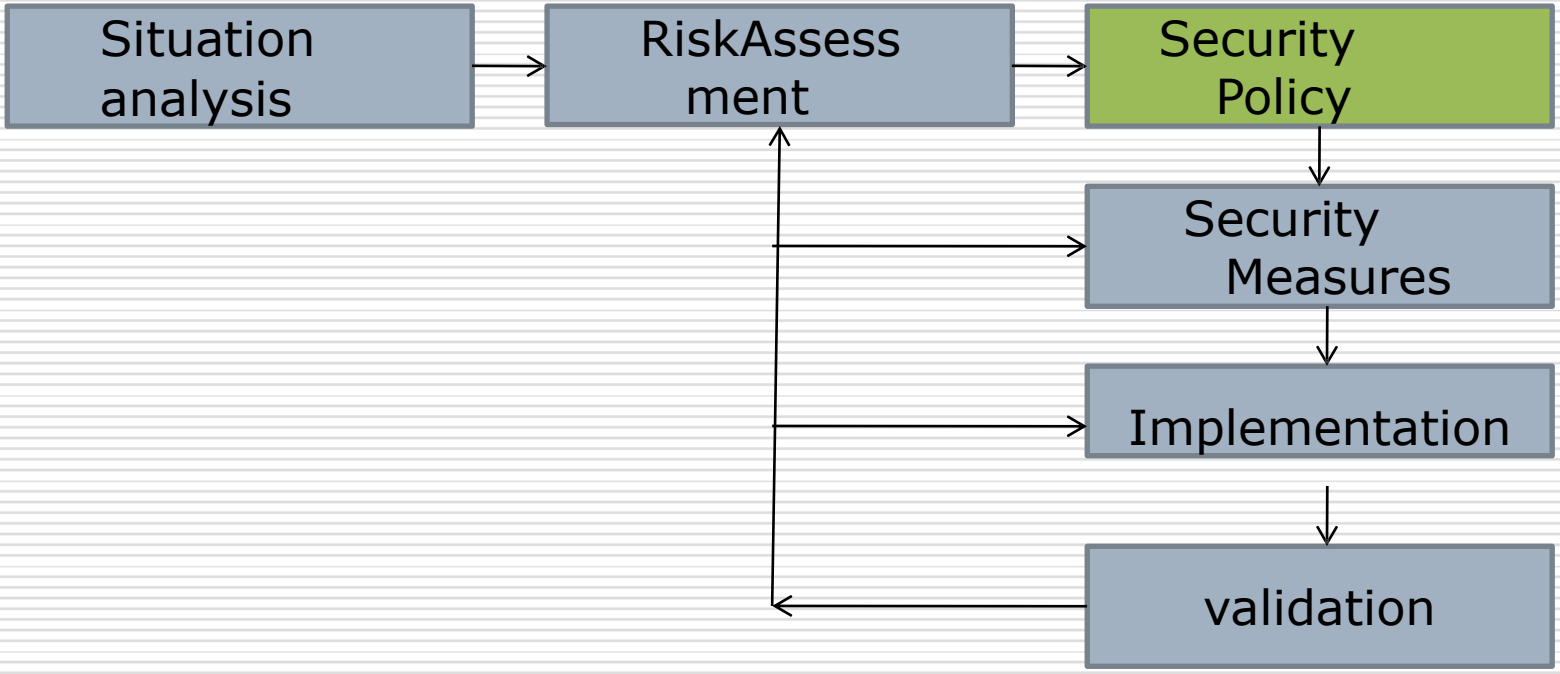
	High Cost	Low Cost
Frequent Incidents	• **Implement security mechanisms** • **Recruit** • **Train...**	Ensure availability (mirror servers, etc.)
Rare Incidents	Ensure	Accept



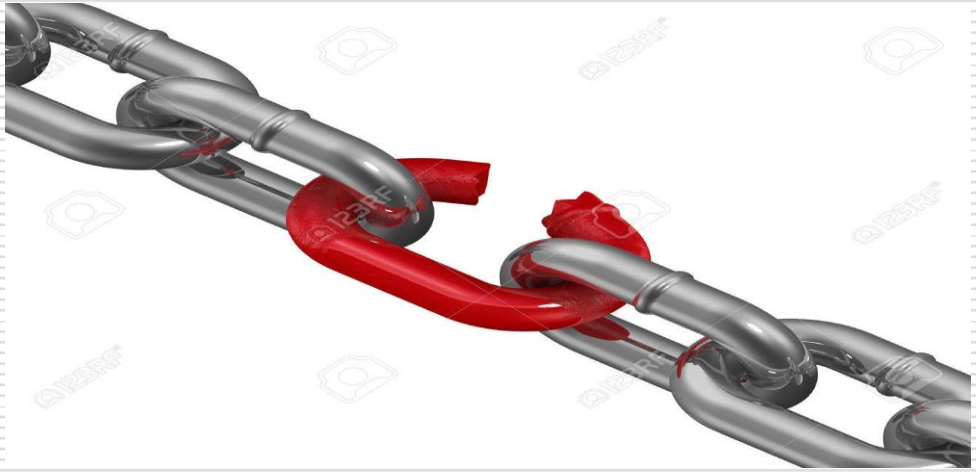
The "zero risk" does not exist, it is necessary to define the residual risk that one is willing to accept.

Establishment of a security policy

Approach (Methodology?) to secure an information system



Approach to securing an IS (Information System) - Establishing a Security Policy



A reinforced door is useless in a building if the windows are open to the street.

Elements of a Security Policy

Approach to securing an IS (Information System) - Elements of a Security Policy

- In addition to ongoing training and awareness for users, the security policy can be divided into several parts:

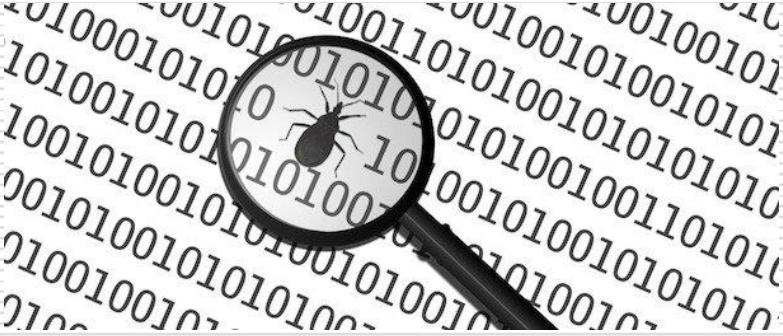
Approach to securing an IS (Information System) - Elements of a Security Policy

- **Hardware failure**

(aging, defects, etc.)

Software failure

(bugs, updates, etc.)



Approach to securing an IS (Information System) - Elements of a Security Policy

- **Accidents (failures, fires, floods, etc.)**

Human error(Training)

Approach (Methodology?) to secure an information system

- **Theft via physical devices Disks,Control access to equipment**

-

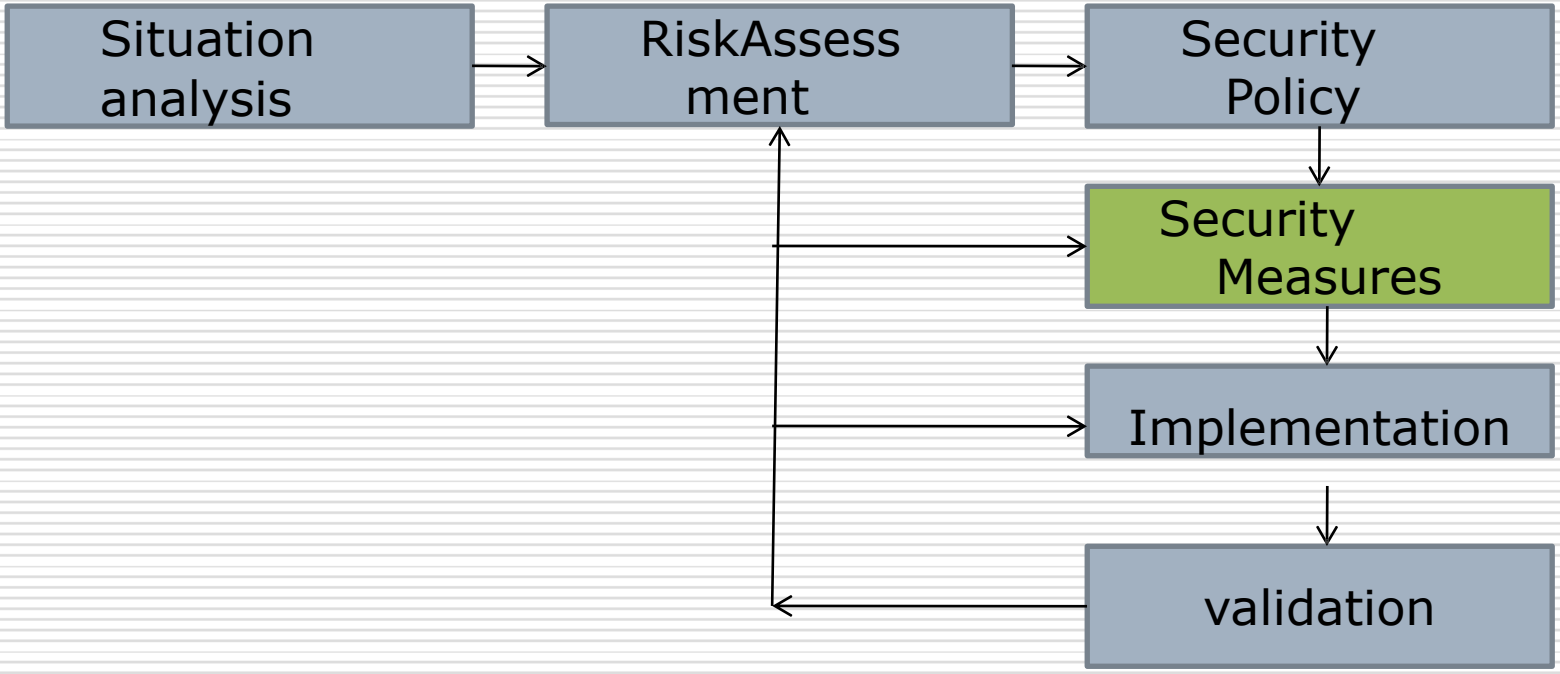
-

- **Viruses from disks**

Approach (Methodology?) to secure an information system

- **Hacking and network viruses (more complex)**

Approach (Methodology?) to secure an information system



Approach (Methodology?) to secure an information system

Technical measures

Firewall,

Antivirus,

IDS,

…

Organizational measures

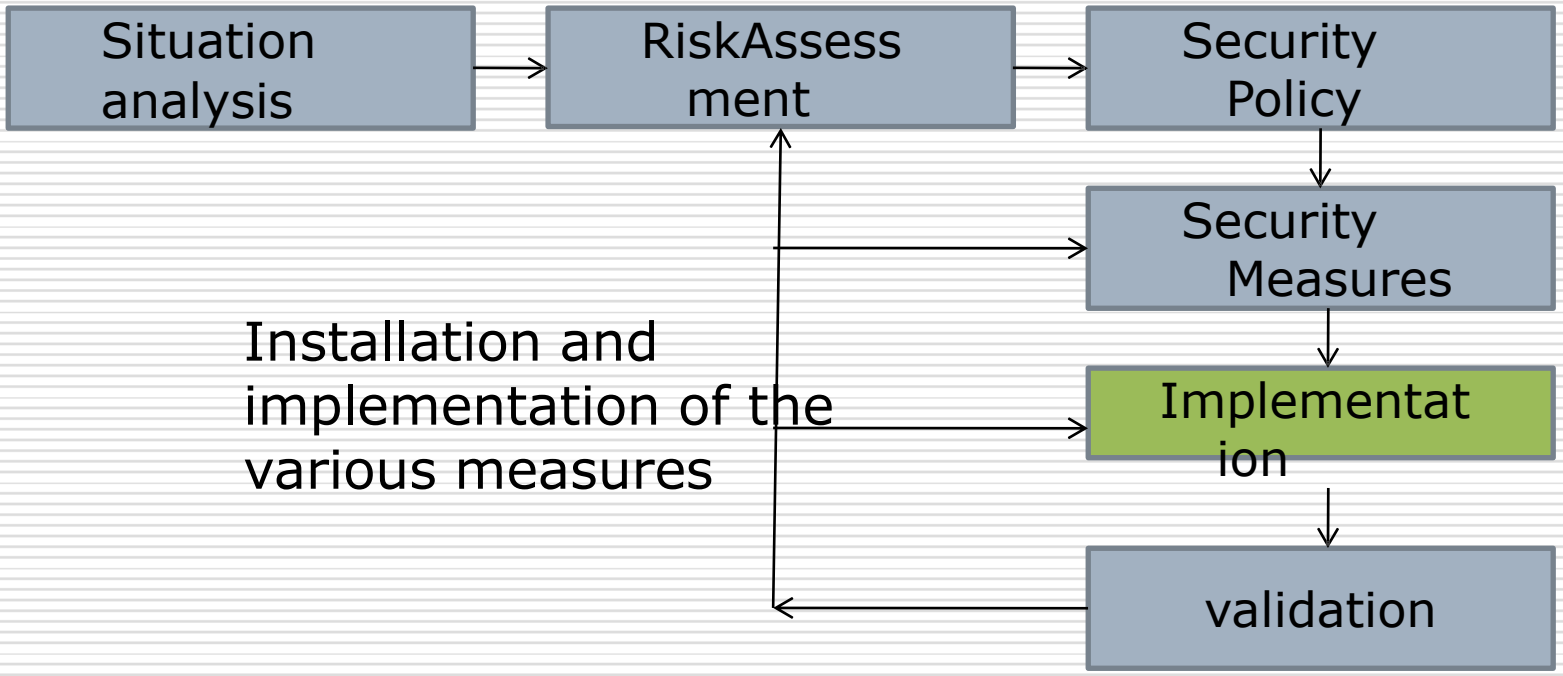
Backup procedures,

appointment of security officer,

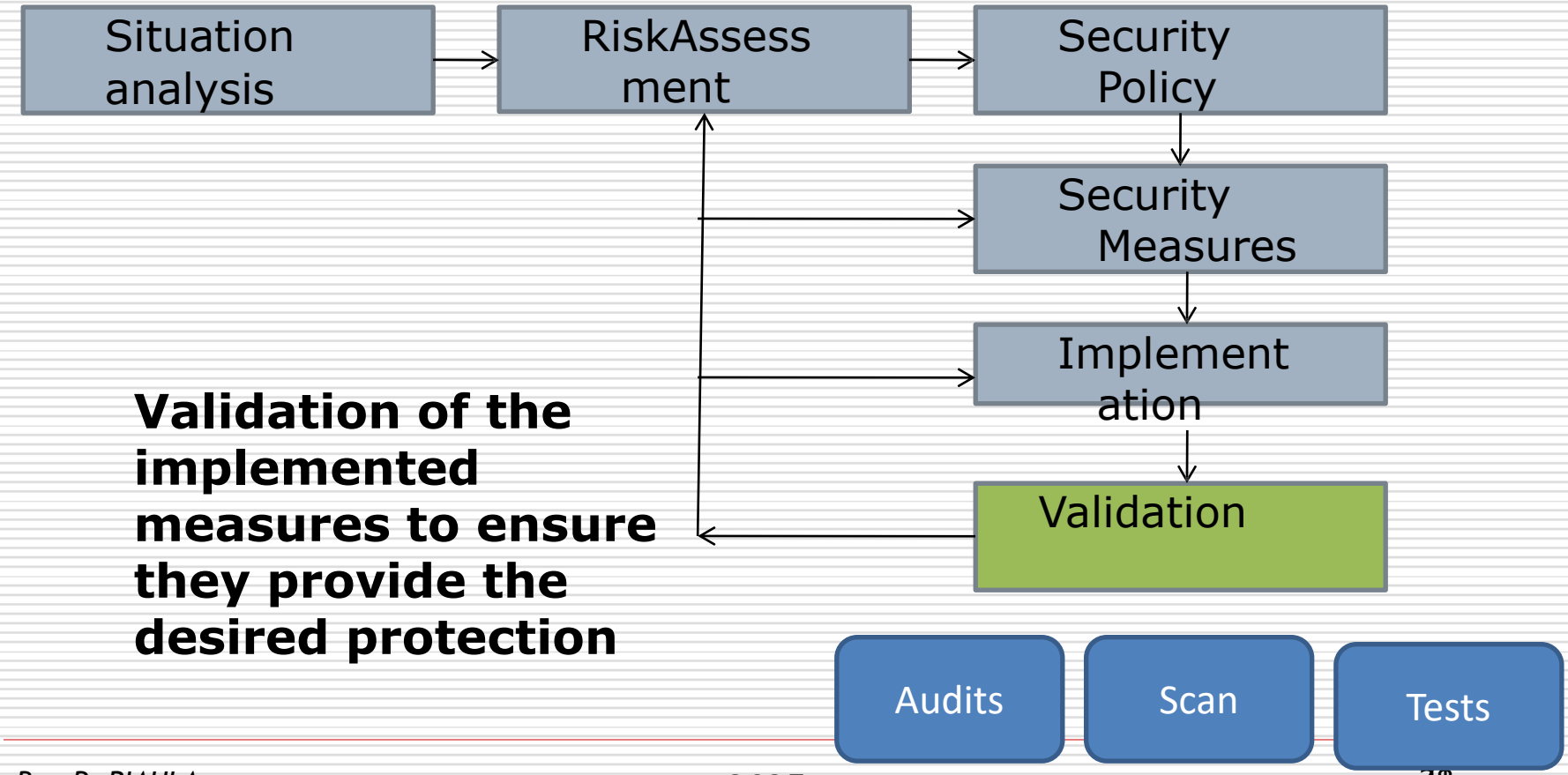
…

<u>To enable the implementation of the security policy</u>

Approach (Methodology?) to secure an information system



Approach (Methodology?) to secure an information system



Validation of the implemented measures to ensure they provide the desired protection

38


SECURITY AUDIT

Audit concept

- A security audit involves relying on a trusted third party (typically a company specialized in cybersecurity) to validate the protective measures implemented, in accordance with the security policy.

- **The goal of the audit is to verify that each rule of the security policy is properly applied and that all the measures taken form a coherent whole.**

Audit concept

A security audit ensures that all the measures taken by the company are considered secure.

END